

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
12 April 2001 (12.04.2001)

PCT

(10) International Publication Number  
**WO 01/26062 A1**

(51) International Patent Classification<sup>7</sup>: **G07F 7/10**

Chandra; 5779 South Winds Drive, Apartment 77, Mentor-on-the-Lake, OH 44060 (US). SHERWIN, Francis, M.; 3377 East Monmouth Road, Cleveland Heights, OH 44118 (US).

(21) International Application Number: PCT/US00/26965

(74) Agent: CORNELY, John, P.; Fay, Sharpe, Fagan, Minnick & McKee, LLP, Seventh floor, 1100 Superior Avenue, Cleveland, OH 44114 (US).

(22) International Filing Date:  
29 September 2000 (29.09.2000)

(81) Designated States (*national*): CA, JP, MX.

(25) Filing Language: English

(84) Designated States (*regional*): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

(26) Publication Language: English

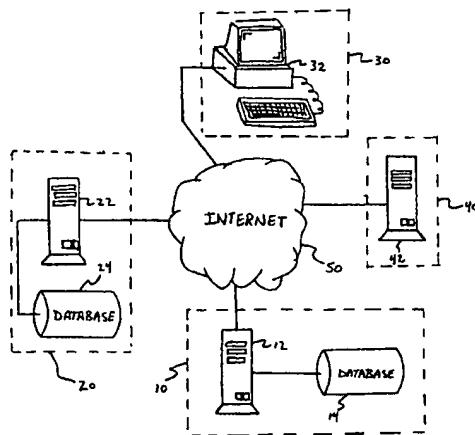
Published:

- *With international search report.*
- *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

(71) Applicant: CARDINALCOMMERCE.COM, INC.  
[US/US]; 6119 Heisley Road, Mentor, OH 44060-1837  
(US).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE AND EFFICIENT PAYMENT PROCESSING SYSTEM



**WO 01/26062 A1**

(57) Abstract: A method of processing secure transactions over unsecure computer networks (50) between account holders (30) and participating merchants (20) includes generating a number of separate periodically changing non-predictable codes, and assigning unique identifiers to a number of account holders (30) such that each identifier is associated with one of the separate periodically changing non-predictable codes. The account holders (30) are provided with tokens (230) that are each synchronized to generate the same periodically changing non-predictable code associated with the unique identifier assigned to the account holder (30) that was provided the token (230). The codes along with identifiers are then received over the unsecure computer network (50) from buyers involved in transactions. For each set of received codes and identifiers, the buyer is authenticated as the account holder (30) having the corresponding identifier when the received code matches the periodically changing non-predictable code for the identifier received.

**SECURE AND EFFICIENT PAYMENT PROCESSING SYSTEM****Background of the Invention**

The present invention is directed to carrying out secure transactions over unsecure computer networks. It finds particular application in conjunction with Internet credit/debit transactions, and will be described with 5 particular reference thereto. However, it is to be appreciated that the present invention is also amenable to other like applications.

Internet commerce, or e-commerce as it is otherwise known, relates to the buying and selling of products and 10 services by buyers and sellers or the transactional exchange of information over the Internet, an unsecure computer network. The convenience of shopping over the Internet has sparked considerable interest in e-commerce on behalf of both buyers and sellers. Internet sales or like transactions have 15 been typically carried out using standard credit/debit cards such as Visa®, MasterCard®, Discover®, American Express®, or the like. However, while widely used for more traditional face-to-face transactions, use of these standard credit/debit cards and their associated processing systems in connection 20 with e-commerce presents certain difficulties.

In particular, for example, standard credit/debit card transactions typically involve a relatively high number of intermediaries that are used in processing the transaction from an initial purchase request, through authentication and 25 authorization, and ultimately to settlement. In addition to the actual buyer and seller, the cast involved in ultimately completing the transaction through to settlement typically entails member banks including a merchant or acquiring bank

-2-

and an issuing bank. Often, an Internet processor (e.g., Cybercash), member service provider (MSP), or an independent sales organization (ISO) is also involved. Additionally, third party processors, agent banks, and/or deposit banks are  
5 commonly employed. As each intermediary charges a bulk, per-transaction, percentage, or other like fee for its role in handling the transaction, the total transaction cost grows with each additional intermediary employed. Consequently, streamlining transaction processing and elimination of  
10 intermediaries beneficially holds transaction costs down.

Another issue is buyer confidence and security. The fact that e-commerce transactions are not carried out face-to-face often creates apprehension in a potential buyer regarding transactions. This apprehension is fueled by  
15 uncertainty of the reputation or quality of seller with whom they're dealing and the security of their credit/debit card information or other personal information (e.g., address, credit card number, phone number, etc.) typically submitted along with a traditional Internet credit/debit transaction.  
20 Additionally, both the credit/debit account holder, sellers, financial institutions are concerned about safeguarding against fraudulent or otherwise unauthorized credit/debit card transactions.

The present invention contemplates a new and  
25 improved transaction processing system and technique for carrying out credit/debit transactions over the Internet that overcomes the above-referenced problems and others.

Summary of the Invention

30 In accordance with one aspect of the present invention, a method of carrying out secure transactions over unsecure computer networks is provided. The method includes generating a number of separate periodically changing non-predictable codes, and assigning unique identifiers to a  
35 number of account holders such that each identifier is associated with one of the separate periodically changing non-predictable codes. The account holders are provided with tokens that are each synchronized to generate the same

-3-

periodically changing non-predictable code associated with the unique identifier assigned to the account holder that was provided the token. The codes along with identifiers are then received over the unsecure computer network from buyers 5 involved in transactions. For each set of received codes and identifiers, the buyer is authenticated as the account holder having the corresponding identifier when the received code matches the periodically changing non-predictable code for the identifier received.

10 In accordance with another aspect of the present invention, a method of conducting secure transactions over an unsecure computer network includes selecting merchants as designated sellers for buyers to perform the secure transactions with. The selected merchants are then provided 15 with transaction objects to be installed on merchant servers connected to the unsecure computer network. The merchant servers are used to perform transactions between the merchants and buyers. Account holders are provided with unique identifiers and tokens. The tokens generate 20 periodically changing non-predictable codes associated with the unique identifiers of the account holders to which the tokens were provided. Likewise, a server connected to the uncesure computer network remotely generates the same periodically changing non-predictable codes associated with 25 each unique identifier. Over the unsecure computer network, sets of information are received associated with transactions due to buyers accessing the transaction objects of selected merchants. Each set of information includes a pass code, and an identifier. Finally, each buyer is authenticated as the 30 account holder having the received identifier when the received pass code matches the remotely generated periodically changing non-predictable code for that identifier.

One advantage of the present invention is that 35 Internet credit/debit transactions are privately, securely, potentially anonymously, and readily carried out.

Another advantage of the present invention is that a high transaction count boosted by increased buyers'

-4-

confidence in Internet shopping leads to increased sales for sellers.

Another advantage of the present invention is that buyers and sellers are protected from fraudulent or otherwise 5 unauthorized transactions.

Yet another advantage of the present invention is that transaction costs are reduced to the extent that streamlined processing reduces intermediaries that would otherwise contribute to the transaction costs.

10 Still further advantages and benefits of the present invention will become apparent to those of ordinary skill in the art upon reading and understanding the following detailed description of the preferred embodiments.

15 Brief Description of the Drawings

The invention may take form in various components and arrangements of components, and in various steps and arrangements of steps. The drawings are only for purposes of illustrating preferred embodiments and are not to be 20 construed as limiting the invention.

FIGURE 1 is a flow chart showing a high level overview of an online credit/debit transaction processing system in accordance with aspects of the present invention;

25 FIGURE 2 is a diagrammatic illustration showing Internet connected participants in an online credit/debit transaction processing system in accordance with aspects of the present invention;

30 FIGURE 3 is a flow chart showing a process for registering sellers for participation in an online credit/debit transaction processing system in accordance with aspects of the present invention;

35 FIGURE 4 is a flow chart showing a process for registering account holders for participation in an online credit/debit transaction processing system in accordance with aspects of the present invention;

FIGURE 5 is a diagrammatic illustration showing a credit token for use in connection with an online

-5-

credit/debit transaction processing system in accordance with aspects of the present invention;

FIGURES 6 and 7 are flow charts showing an online shopping experience and related processing in accordance with 5 aspects of the present invention with pre-shopping authentication and post-shopping authentication, respectively;

FIGURE 8 is a flow chart showing implementation of additional security measures invoked by certain delivery 10 destination conditions which are selected in connection with an online credit/debit transaction processing system in accordance with aspects of the present invention;

FIGURE 9 is a flow chart showing a settlement process of an online credit/debit transaction processing 15 system in accordance with aspects of the present invention; and,

FIGURE 10 is a flow chart showing a micro-payment processing application of an online credit/debit transaction 20 processing system in accordance with aspects of the present invention.

#### Detailed Description of the Preferred Embodiments

With reference to FIGURE 1, a central transaction coordinator 10 administers a number of different yet inter-dependent processes in a commercial Internet credit/debit transaction processing system A. The processes administered by the coordinator 10 include: (i) a seller registration process 100 wherein merchants or sellers are signed up for participation in the transaction processing system A; (ii) an account holder registration processes 200 wherein buyers or consumers are signed up as account holders for participation in the transaction processing system A; (iii) an online shopping process 300 wherein buyers or consumers engage in online commercial transactions with merchants or sellers; 35 and, (iv) a settlement process 400 wherein completed commercial transactions are confirmed and settlement information forwarded directly to a funding source for billing and payment processing. Optionally, the coordinator

-6-

10 also administers a micro-payment process 500 wherein individual small transactions (i.e., transactions involving funds that are less than or small relative to any associated processing fees or costs) are aggregated prior to the 5 submission of settlement information to the funding source. In addition, the coordinator 10 itself optionally acts as the funding source. However, in the interest of simplicity and clarity, in the following description, the discussion is directed to embodiments employing a third party funding 10 source.

With further reference to FIGURE 2, in a preferred embodiment, the coordinator 10 maintains a presence on the Internet 50 or other like online network via a server 12. A merchant or seller 20 also maintains a presence on the 15 Internet 50 via a server 22. A buyer or account holder 30 gains access to the seller 20 and/or the coordinator 10 over the Internet 50 using a computer 32 with an appropriate web browser or other like software running thereon. Of course, the transaction processing system A is preferably 20 administered to multiple similarly situated sellers 20 and buyers 30. However, in the interest of simplicity herein, only a one of each are shown in FIGURE 2. Additionally, a funding source 40 maintains a presence on the Internet 50 via a server 42. The funding source 40 extends credit for credit 25 accounts or holds deposits for debit accounts created on behalf of account holders participating in the transaction processing system A. Moreover, it is to be appreciated that the security of the transaction processing system A is further enhanced by encrypting, with known encryption 30 techniques, communications relayed or otherwise transmitted over the Internet 50.

With further reference to FIGURE 3, in the seller registration process 100, an interested merchant or seller 20, preferably doing business on the Internet 50 via their 35 server 22, is registered for participation in the Internet credit/debit transaction processing system A administered by the transaction coordinator 10. The seller registration process 100 begins with the coordinator 10 receiving seller

-7-

information 102 (e.g., financial information, physical address, category of good or services sold, Internet address, e-mail address, etc.) from the seller 20. Online or over the Internet 50, this is optionally accomplished by receiving the 5 seller information 102, perhaps encrypted, via the coordinator's server 12. Using the received seller information 102, the worthiness of the seller 20 for participation in the Internet credit/debit transaction processing system A is evaluated.

10 Preferably, a verification program 110 is applied to evaluate the seller 20 based on the seller information 102 received by the coordinator 10. The verification program 110, optionally running on the coordinator's server 12, is carried out using a predetermined or otherwise selected 15 algorithm that acts on quantifiable values representing the seller information 102. In this manner, the seller's credit worthiness is determined and/or the seller's reliability and reputation for customer service and sound business practice is determined using objective, subjective, or a combination 20 of objective and subjective criteria. Accordingly, the coordinator 10 ensures that the seller 20 is able to meet potential obligations. Moreover, account holders 30 participating in the transaction processing system A are reassured that they are patronizing high quality merchants or 25 sellers with strong customer satisfaction guarantees.

In response to the evaluation, at decision step 120, the coordinator 10 decides whether or not the interested seller 20 is declined or approved for participation. If declined, a notification 122 is sent to the interested seller 30 20 and the seller registration process 100 ends. If approved, the coordinator 10 forwards a seller agreement 124 to the seller 20. Online or over the Internet 50, the seller agreement 124 is optionally forwarded from the coordinator's server 12 to the seller's server 22. The seller agreement 124 35 outlines the rights and responsibilities or duties of the seller 20 with respect to their participation in the credit/debit transaction processing system A. After the seller 20 physically signs, electronically signs, or

-8-

otherwise executes the seller agreement 124, it is returned to the coordinator 10, perhaps through the coordinator's server 12. Upon receipt of the executed seller agreement 124a, the coordinator 10 creates and maintains a record of 5 the seller information 102, the seller's approval, the seller agreement 124, etc. Preferably, the record is electronically created and maintained in a coordinator's database 14 which is accessible by the coordinator 10, and optionally, the funding source 40.

10           Preferably, upon acceptance of the executed seller agreement 124a, the coordinator 10 forwards to the seller 20 a transaction object 126 which places a link on the seller's online shopping check-out page or otherwise runs on the seller's server 22. The object or link operates to integrate 15 the credit/debit transaction processing system A into, or otherwise allows the processing system A to be accessed through, the seller's online shopping system or Internet shopping web page or pages. Optionally, the coordinator 10 installs the object on the seller's server 22. Accordingly, 20 account holders 30 shopping online or over the Internet 50 can access the object (e.g., by clicking the link on seller's check-out web page) and be automatically routed to the coordinator 10 for authentication and/or authorization. In this manner then, merchants or sellers 20 become registered 25 for participation in the transaction processing system A.

With further reference to FIGURE 4, in the account holder registration process 200, registration of a buyer or consumer to become an account holder 30 begins with a visit by the buyer to the coordinator 10. Optionally, over the 30 Internet, the interested buyer or consumer, using an appropriate web browser, accesses an account holder registration page which is made available via the coordinator's sever 12. As the account holder registration process 200 continues, account holder registration data 202 35 (e.g., name, address, length at residence, own or rent residence, e-mail address, home phone number, work phone number, social security number, date of birth, mother's maiden name, employer, income, employment status, etc.) is collected

-9-

or otherwise obtained by the coordinator 10 from the buyer or the potential new account holder 30 who is making application for participation in the credit/debit transaction processing system A. Prior to accepting the consumer or buyer as a new 5 account holder 30, their credit worthiness is evaluated.

Preferably, the coordinator 10 passes relevant account holder registration data 202 to the funding source 40. The relevant account holder registration data 202 is then analyzed for credit worthiness. Optionally, the data is 10 analyzed by the funding source's own credit approval system, or it is passed on to one or more credit bureaus 210 for analysis. The analysis preferably includes the application of known credit approval techniques and algorithms which determine credit worthiness. Ultimately, credit approval 15 data 212 (e.g., approval or denial, amount of credit, risk, etc.) is routed back to the coordinator 10 through the funding source 40.

Upon receipt of the credit approval data 212, the coordinator 10 decides, at decision step 220, if the 20 potential new account holder 30 is worthy of participation in the transaction processing system A. Then the coordinator 10 notifies the potential new account holder 30 of the credit decision. That is to say, if credit is declined, a credit-declined message 222 is communicated to the potential account 25 holder 30. On the other hand, if credit is approved, approval information 224 (e.g., the annual percentage rate, credit limit, etc.) is communicated to the potential new account holder 30 for acceptance. In a preferred embodiment, the credit approval or denial is communicated to an online 30 potential new account holder 30 accessing the coordinator over the Internet 50 by displaying an appropriate web page from the coordinator's server 12 to the potential new account holder 30. Alternately, the credit approval or denial is communicated via e-mail to the potential new account holder's 35 designated e-mail address previously obtained along with the account holder registration data 202. In any event, optionally, at this time, the potential new account holder 30 is advanced an initial, albeit preferably limited, line of

-10-

credit and temporary password enabling him to immediately shop online at a registered seller 20 using the credit/debit transaction processing system A administered by the transaction coordinator 10.

5        If approved and account holder status is still desired, along with an indication of acceptance, the account holder 30 supplies the coordinator 10 with additional account creation data 226 including a secret personal identification number (PIN) and the answers to a number of designated or  
10 otherwise selected security questions. The security questions are preferably questions to which only the account holder 30 is likely to know the answers (e.g., the account holder's first car, the name of the account holder's dog, etc.). Upon acceptance, the coordinator 10 creates and  
15 maintains a record for the account holder 30, preferably in electronic format on the coordinator's database 14. The account holder record includes the account holder registration data 202, credit approval data 212, approval information 224, acceptance, and additional account creation  
20 data 226. In addition, a corresponding credit account is created with the funding source 40.

      The account holder record may also contain information or data relating to account privileges. In a preferred embodiment the account holder 30 has the option to  
25 customize or modify their account privileges. The account privileges are customized by the account holder 30, for example, by accessing the coordinator's server 12 over the Internet 50. For security purposes, the account holder is optionally authenticate as such, preferably, using the below  
30 described authentication procedure, prior to permitting any account modifications. However, at initial account creation, the below described authentication procedure is not employed. The account privileges are optionally set by the account holder 30 to limit the use of the account holder's account in  
35 the transaction processing system A. That is to say, the set account privileges may restrict the account so that purchases thereon are not authorized for specified participating merchants or sellers 20, so that automatically recurring

-11-

transactions carried out absent the direct participation of the account holder 30 are not authorized, so that single purchases over a certain price limit are not authorized, so that aggregate per day purchases are limited to a desired 5 level, and the like.

At the initial account creation, the coordinator 10 also assigns the account holder 30 an associated user identity which is unique to the account holder 30 and becomes part of the account holder's record (e.g., a self-selected 10 user name, or an otherwise assigned alpha-numeric designation), and optionally, a corresponding credit token 230 (see FIGURE 5) is issued to the account holder 30. The credit token 230 periodically (e.g., every 60 seconds) generates a non-predictable alpha-numeric code (preferably 6 15 characters in length) using a predetermined or otherwise selected algorithm. The algorithm used in generating the periodically changing non-predictable alpha-numeric code is preferably a function of an initial seed value and a time value obtained from an internal clock. The credit token 230 20 renders the code on an incorporated liquid crystal display (LCD) readout 232 or other like human-viewable display. Additionally, the credit token 230 provides an indicator as to the duration of the displayed code's validity (i.e., the time remaining before generation of the next non-predictable 25 code). Accordingly, every period, the credit token 230 generates a dynamically changing non-predictable alpha-numeric code which (with the exception of the coordinator 10) is only available to the account holder 30 in possession of the credit token 230.

For each unique user identity, the coordinator 10 30 also independently generates a periodically changing non-predictable alpha-numeric code which is synchronized with and the same as the token generated code for the corresponding account holder 30 having that user identity. The independently generated and synchronized code is 35 maintained with the corresponding account holder's record. Preferably, the coordinator 10 generates the synchronized code by running software which uses (i) an algorithm and (ii)

-12-

an initial seed value which are both identical to that used by the corresponding token 230 and (iii) a time value from a clock which is synchronized with the token's internal clock. In this manner then, the alpha-numeric code from an account holder's credit token 230 and the independently generated alpha-numeric code maintained with the account holder's record are the same at any given time.

Alternately, a potential new account holder 30 may contact the funding source 40 directly for registration to participate in the transaction processing system A. In this case, the funding source carries out substantially the same account holder registration process 200 and forwards the account holder record to the coordinator 10.

With further reference to FIGURES 6 and 7, in a preferred embodiment, an online or Internet shopping experience or process 300 begins with an account holder 30 contacting the coordinator 10 (e.g., accessing the coordinator's online or Internet shopping portal using an appropriate web browser) or otherwise requesting a web page from or linking to the coordinator's server 12. At this juncture, the account holder 30 is given the option to pre-authenticate their identity prior to engaging in any particular commercial transactions with the participating merchants or sellers. Authentication is preferably accomplished by the coordinator 10 collecting from the account holder 30 authentication data 302 having one or more elements including the account holder's user identity, PIN, and/or token generated alpha-numeric code. Optionally, one or more elements of the authentication data 302 are entered manually by the account holder 30. Alternately, one or more of the elements are stored or otherwise maintained on the computer 32 being employed by the account holder 30 to access the coordinator's server 12 such that they are automatically entered where appropriate. For example, with regard to the non-predictable alpha-numeric code, rather than having a separate physical token 230, the "token" is optionally an object running on the account holder's computer 32 which enters or displays the alpha-numeric code when accessed.

-13-

Alternately, a separate physical token 230 optionally includes an interface 234 (see FIGURE 5) through which it is connected to the account holder's computer such that the token generated alpha-numeric code is read directly from the token 5 230 without manual entry.

In any event, the coordinator 10 runs the authentication data 302 through an authentication process 310 which compares the entered or otherwise collected authentication data 302 with the corresponding data in the 10 account holder record having the same user identity as that included with the authentication data 302. The coordinator 10 then determines, at decision step 320, whether or not the alleged account holder 30 is an authentic account holder previously registered using the account holder registration 15 process 200. Of course, where the user identity included with the authentication data 302 does not have a corresponding account holder record or is otherwise invalid, the authentication is denied or fails and the alleged account holder 30 and/or involved seller 20 is sent a denial 20 notification 322. Additionally, where the authentication data 302 and corresponding data in the account holder record having the same user identity do not match, the authentication is also denied or fails and the alleged account holder 30 and/or involved seller 20 is again sent the 25 denial notification 322. Only when there is an identical match between the authentication data 302 and the account holder record does the accessing account holder 30 become authenticated and/or positively identified as the true account holder having the corresponding user identity.

30 Alternately, various authentication methods or procedures are employed such that there is a positive identification of the account holder 30. Examples of such authentication procedures include, challenge response, quick log mode, other one or more factor authentication methods 35 (such as a static user name and password or PIN), smart cards, biometric authentication (such as fingerprint recognition or retinal scanners), etc. These authentication techniques ensure that the coordinator 10 is able to

-14-

independently make a positive identification of the account holders 30.

With particular reference now to FIGURE 6, next, the account holder 30 requests, or the coordinator's server 12 otherwise displays, a web page or the like with a shopping directory 330 listing participating merchants or sellers 20 that are registered with the credit/debit transaction processing system A system administered by the coordinator 10. The account holder 30 is then free to select the participating seller 20 of his choice and shop as a pre-authenticated account holder 30a.

With particular reference now to FIGURE 7, alternately, the account holder 30 accesses the seller's online store or Internet shopping site directly from the seller's server 22 and shopping is carried out absent pre-authentication. At the seller's site, the buyer or account holder 30 selects items 340 of goods and/or services which are desired for purchasing. Preferably, these goods or services are then placed into a virtual shopping cart 342. If more shopping is desired, the process loops back to product selection and other like shopping web pages made available from the seller's server 22. On the other hand, if shopping is complete, the process continues on to check-out 350. When the buyer or account holder 30 accesses the transaction object 126 or link previously established on the participating merchant's or seller's check-out page 350, the buyer or account holder 30 is routed to the coordinator 10 along with a purchase request 352 indicating the buyer desires to carry out a commercial transaction with the referring participating seller 20. Preferably, the transaction in question includes the buyer or account holder 30 purchasing one or more selected items from the participating merchant or seller 20.

If not pre-authenticated, when the buyer or account holder 30 is routed to the coordinator 10, they are presented with an authentication page from the coordinator's server 12. At this point, using the same authentication procedure 310 as used in pre-authentication, the buyer is authenticating

-15-

and/or positively identified as an account holder 30 having a unique user identity. If pre-authenticated, the account holder 30 bypasses this authentication step.

In any event, provided authentication is complete  
5 and successful, the coordinator 10, at process step 360, establishes transaction fulfillment data 362. The transaction fulfillment data 362 identifies information which is used by the participating seller 20 to fulfill their obligation(s) to the account holder 30 for the commercial  
10 transaction in which they are currently engaged. For example, the transaction fulfillment data 362 preferably includes a delivery destination for the items selected for purchase in the transaction. For physical goods, the delivery destination may be a shipping address, and for  
15 downloaded content, downloaded software, digital goods or services, and other like items, the delivery destination may be an e-mail address or the account holder's networked computer 32.

With further reference to FIGURE 8, in a preferred  
20 embodiment, previously designated (e.g., at account creation) default delivery destinations for the various types of goods or services are maintained in the account holder's record. As a rule, the coordinator 10 uses these default designations in establishing the transaction fulfillment data 362. However,  
25 at a destination selection web page 364 presented to the account holder 30 by the coordinator 10, the account holder 30 may optionally designate, via a selection response 366, an alternate destination as the delivery destination.

In a preferred embodiment, if the alternate  
30 destination differs from the default destination or if the destination is a direct download to the buyer's or account holder's computer 32, an additional security precaution is invoked. More specifically, the coordinator 10 transmits one or more of the previously answered security questions 226a  
35 (i.e., the security questions to which the account holder 30 originally provided answers in connection with the submitted additional account creation data 226) to the buyer or account holder 30. The coordinator 10 then receives from the buyer

-16-

or account holder 30 an answer 226b in response to each security question. The coordinator 10 then determines, at decision step 370, if the answers 226b are correct. As shown at process step 372, only when the newly received responses 5 match the previously given answers in the account holder's record is the alternate or download destination included in the established transaction fulfillment data 362. Otherwise, as shown at process step 374, the alternate or download destination is rejected. Optionally, approved alternate 10 destinations may also be stored in an account holder address book maintained with the account holder's record for convenient future access and use by the account holder 30.

Optionally, the delivery destination is a non-identifying destination such that anonymity of the account 15 holder 30 is maintained with respect to the participating merchant or seller 20. For example, the non-identifying destination may be a post office box, or other neutral third party from which delivered goods are obtained by the account holder 30. Regardless of the delivery destination, once 20 established, the transaction fulfillment data 362 is communicated by the coordinator 10, preferably online or over the Internet 50, to the participating seller 20, and the account holder 30 is routed back the participating seller 20 where they are optionally presented a shipping choice 380 25 including choice of shipping carrier (e.g., regular U.S. mail, Federal Express, UPS, etc.) and/or preferred shipping time (e.g., 1 month, 1 week, or next day delivery).

After the account holder 30 has made their selection 382, if any, with regard to shipping carrier and/or 30 preferred shipping time, the transaction details 384 are transmitted from the seller 20 to the coordinator 10 where they are received for authorization processing 390. The transaction details 384 preferably include the total cost 35 (with tax and shipping) for the selected items being purchased in the transaction. Additionally, the transaction details 384 identify the participating merchant or seller 20 and account holder 30 engaged in the transaction. Authorization is based upon the account holder's credit

-17-

account having an amount of available credit sufficient to cover the total cost of the transaction. Alternately, the account is optionally a debit account such that authorization is based upon the debit account having a sufficient amount of 5 funds on deposit to cover the total cost of the transaction. In either case, when a sufficient amount of funds or credit is available to cover the total cost of the transaction, completion of the transaction is authorized, if not authorization is denied.

10        Optionally, the status of the account holder's account (credit or debit) is maintained along with the account holder's record in the coordinator's database 14 such that the coordinator 10 may directly authorize transactions. Alternately, the transaction details 384 are passed along to 15 the fund source which then authorizes the transactions. In either case, upon determining authorization (in the affirmative or in the negative), a corresponding authorization code 392 is established for the transaction. Preferably, the authorization code 392 along with the 20 authorization result and the corresponding transaction details 384 are maintained in a transaction record, optionally, stored electronically in the coordinator's database 14. Additionally, an indication of the authorization outcome and the authorization code 392 are 25 communicated to the participating merchant or seller 20 and account hold 30 which then act accordingly.

With further reference to FIGURES 9, the settlement process 400 for completed commercial transactions begins with the coordinator 10 collecting or otherwise obtaining 30 settlement information 402 from the seller 30. Preferably, the settlement process 400 occurs periodically, e.g., daily, weekly, etc. Alternately, the settlement information 402 is obtained by the seller 20 routing settlement information 402 to the coordinator 10 or by the coordinator 10 automatically 35 extracting settlement information 402 from the seller 20. For example, with regard to the automatic extraction of settlement information, when a seller's delivery process is executed thereby delivering purchased goods or services to

-18-

the account holder 30, a seller's inventory database 24 (see FIGURE 2) or other such seller database is accordingly updated to indicate delivery and completion of the particular transaction. In the settlement procedure 400 then, 5 settlement information 402 corresponding to those transactions indicated in the seller's database 24 as having been completed is automatically retrieved by the coordinator 10 from the seller's database 24.

The settlement information 402 indicates that the 10 seller 20 has fulfilled his obligations to an account holder 30 in connection with a particular authorized commercial transaction. The obtained settlement information 402 preferably includes the authorization code 392 and the corresponding transaction details 384 for the transaction in 15 question. The coordinator 10 then matches the settlement information 402 to the corresponding transaction record having the same authorization code 392 to confirm or otherwise validate and approve settlement when the transaction details 384 in the settlement information 402 are 20 substantially the same as the transaction details 384 in the transaction record. In particular, the total cost from the transaction details 384 reported in the settlement information 402 is optionally permitted to vary within a given tolerance from the total cost contained in the 25 transaction details 384 of the transaction record. In the cases where there is an insufficient match, rejected settlement information 402a is returned to the seller 20.

In a preferred embodiment, periodically (e.g., at the end of each day), the coordinator 10 communicates 30 confirmed settlement information 402b directly to the funding source 40, preferably over the Internet 50 or other online network. In turn, the funding source 40 acts accordingly on the confirmed settlement information 402b, e.g., sending bills 410 to the appropriate account holders 30 and 35 reimbursing the appropriate merchants or sellers 20 with payment 420 using known billing and payment processing procedures and methods. As the settlement information 402 has already been confirmed by the coordinator 10, optionally,

-19-

the funding source 40 does not employ independent confirmation of the settlement information 402 and thus may act on the confirmed settlement information 402b more readily without additional procedures for validating it.

5        In this manner, transactions conducted in the transaction processing system A are streamlined as compared to traditional transaction processing systems. In the traditional system, buyers or account holders make purchases using a traditional credit card. The credit card number, 10 expiration date, and accompanying personal information is then forwarded to numerous different intermediaries in an attempt to positively identify and/or authenticate the buyer as the credit card owner. Still further intermediaries are often employed to then authorize a particular transaction and 15 the information is again routed to these additional intermediaries. As a result this system is inherently inefficient. In the transaction processing system A described herein, by providing positive user identification and/or authentication at check-out through the coordinator 10 20 and by integrating the authentication and authorization procedures 310 and 390, respectively, with the coordinator 10, desirable efficiencies are gained insomuch as the inefficient merchant banking system and the numerous intermediaries are avoided on both the purchase side and the 25 settlement side.

With further reference to FIGURE 10, in a preferred embodiment, an account holder 30 is given the option to activate a micro-payment account, for example, by charging their micro-payment account with a minimum predetermined 30 amount (e.g., \$25). Once the micro-payment account is activated, the account holder 30 can use the micro-payment account at a seller's site to purchase goods and services involving small transaction amounts. The authentication process and authorization remains the same as that used for 35 standard transactions. However, the individual micro-payment transactions are held and aggregated by the coordinator 10 prior to being sent to the funding source 40 for settlement. As with the standard transactions, the micro-payment

-20-

transaction details are maintained by the coordinator 10 for future use in settlement. Based on predetermined or otherwise selected criteria, the cumulative settlement information is sent from coordinator 10 directly to the 5 funding source 40 when the cumulative transaction amount is sufficiently greater than applicable processing fees or costs. Accordingly, this process allows the coordinator 10 to aggregate micro-payment transactions to limit the number of settlement transactions thus reducing the per-transaction 10 processing fees or costs. Upon depletion of the account holder's micro-payment account, the account holder 30 is instructed to re-charge their micro-payment account, preferably, in set monetary increments, e.g., \$25, \$50, or the like. The micro-payment account may be considered 15 depleted whenever the balance is insufficient to cover a micro-payment transaction.

In addition to administering the transaction processing system A for registered participants, the coordinator 10 also optionally opens the system up to outside 20 third parties such as private label credit card issuers. In this manner, the transaction processing system A acts as a universal platform from which the private label cards can be used to conduct commercial transactions outside the issuer's store.

25 The invention has been described with reference to the preferred embodiments. Obviously, modifications and alterations will occur to others upon reading and understanding the preceding detailed description. For example, the transaction processing system A is equally 30 applicable to and adept at handling face-to-face transactions, telephone transactions, and the like, as it is at handling Internet transactions. It is intended that the invention be construed as including all such modifications and alterations insofar as they come within the scope of the 35 appended claims or the equivalents thereof.

-21-

Having thus described the preferred embodiments,  
the invention is now claimed to be:

1. A method of carrying out secure transactions over unsecure computer networks, said method comprising:
  - (a) generating a number of separate periodically changing non-predictable codes;
  - 5 (b) assigning unique identifiers to a number of account holders, each identifier being associated with one of the separate periodically changing non-predictable codes;
  - (c) providing the account holders with tokens;
  - (d) synchronizing the tokens with step (a) such
- 10 that each token generates the same periodically changing non-predictable code associated with the unique identifier assigned to the account holder being provided the token;
- (e) receiving codes along with identifiers over the unsecure computer network from buyers involved in
- 15 transactions; and,
- (f) for each set of received codes and identifiers, authenticating the buyer as the account holder having the corresponding identifier when the received code matches the periodically changing non-predictable code for
- 20 the identifier received.

2. The method according to claim 1, wherein each separate periodically changing non-predictable code is a string of alpha-numeric characters.
3. The method according to claim 2, wherein there are at least 6 alpha-numeric characters in each string.
4. The method according to claim 1, said method further comprising:
  - 5 displaying in a human-viewable format the periodically changing non-predictable codes generated by each token.

-22-

5. The method according to claim 4, said method further comprising:

indicating an amount of time remaining until a next change of the periodically changing non-predictable codes.

6. The method according to claim 1, said method further comprising:

(g) authorizing completion of the transaction when the buyer has been authenticated as the account holder; and,

5 (h) denying authorization for completion of the transaction when the buyer has not been authenticated as the account holder.

7. A method of conducting secure transactions over an unsecure computer network, said method comprising:

(a) selecting merchants as designated sellers for buyers to perform the secure transactions with;

5 (b) providing the selected merchants with transaction objects to be installed on merchant servers connected to the unsecure computer network, said merchant servers being used to perform transactions between the merchants and buyers;

10 (c) providing account holders with unique identifiers and tokens;

(d) generating with the tokens periodically changing non-predictable codes associated with the unique identifiers of the account holders to which the tokens were

15 provided;

(e) remotely generating with a server connected to the uncesure computer network the same periodically changing non-predictable codes associated with each unique identifier;

20 (f) receiving, over the unsecure computer network, sets of information associated with transactions due to buyers accessing the transaction objects of selected merchants, each set of information including a pass code, and an identifier; and,

25 (g) authenticating each buyer as the account holder having the received identifier when the received pass

-23-

code matches the remotely generated periodically changing non-predictable code for that identifier.

7. The method according to claim 6, wherein when the set of information received includes an identifier that has not been provided to any account holder, authentication is denied.

8. The method according to claim 6, said method further comprising:

prior to step (c), obtaining personal information about each account holder; and,

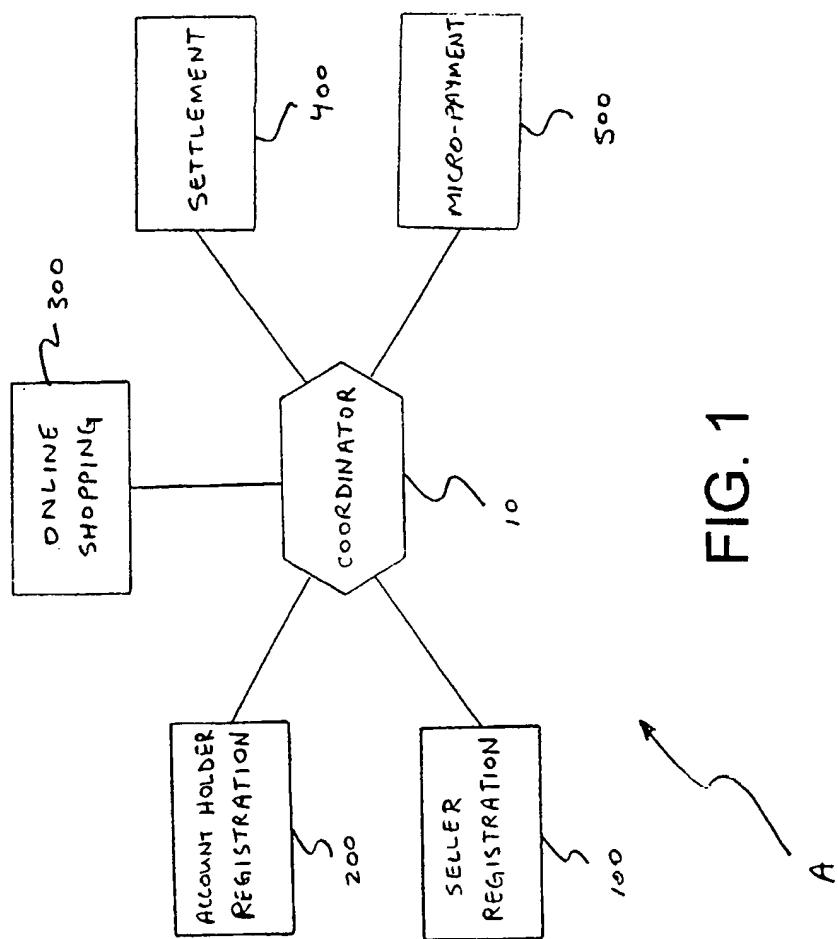
5 after step (g), communicating to merchants the personal information of account holders corresponding to authenticated buyers.

9. The method according to claim 8, wherein for each account holder the obtained personal information includes an account holder address.

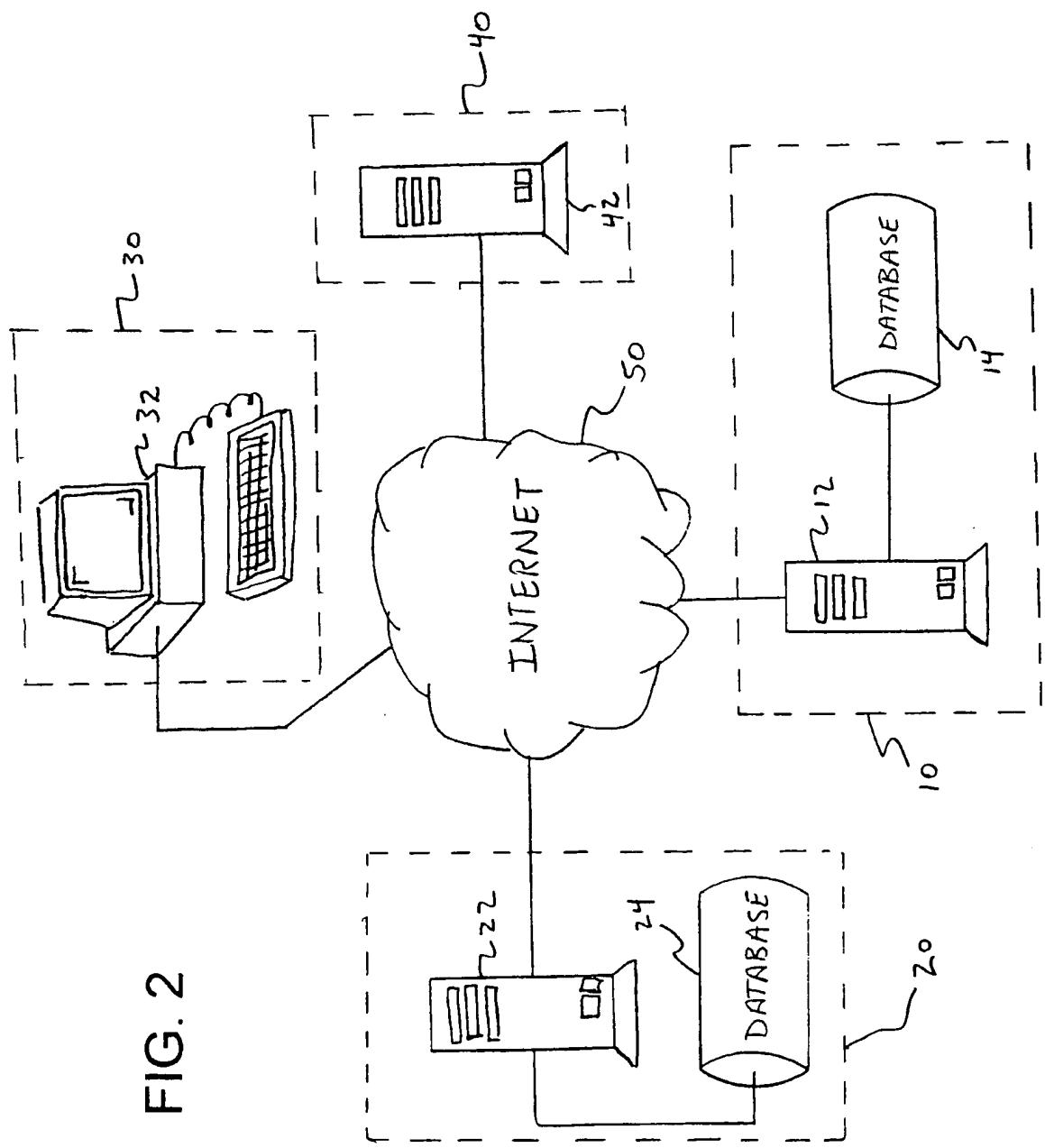
10. The method according to claim 6, said method further comprising:

(h) authorizing completion of the transaction when the buyer has been authenticated as the account holder; and,

5 (i) denying authorization for completion of the transaction when the buyer has not been authenticated as the account holder.



2/10



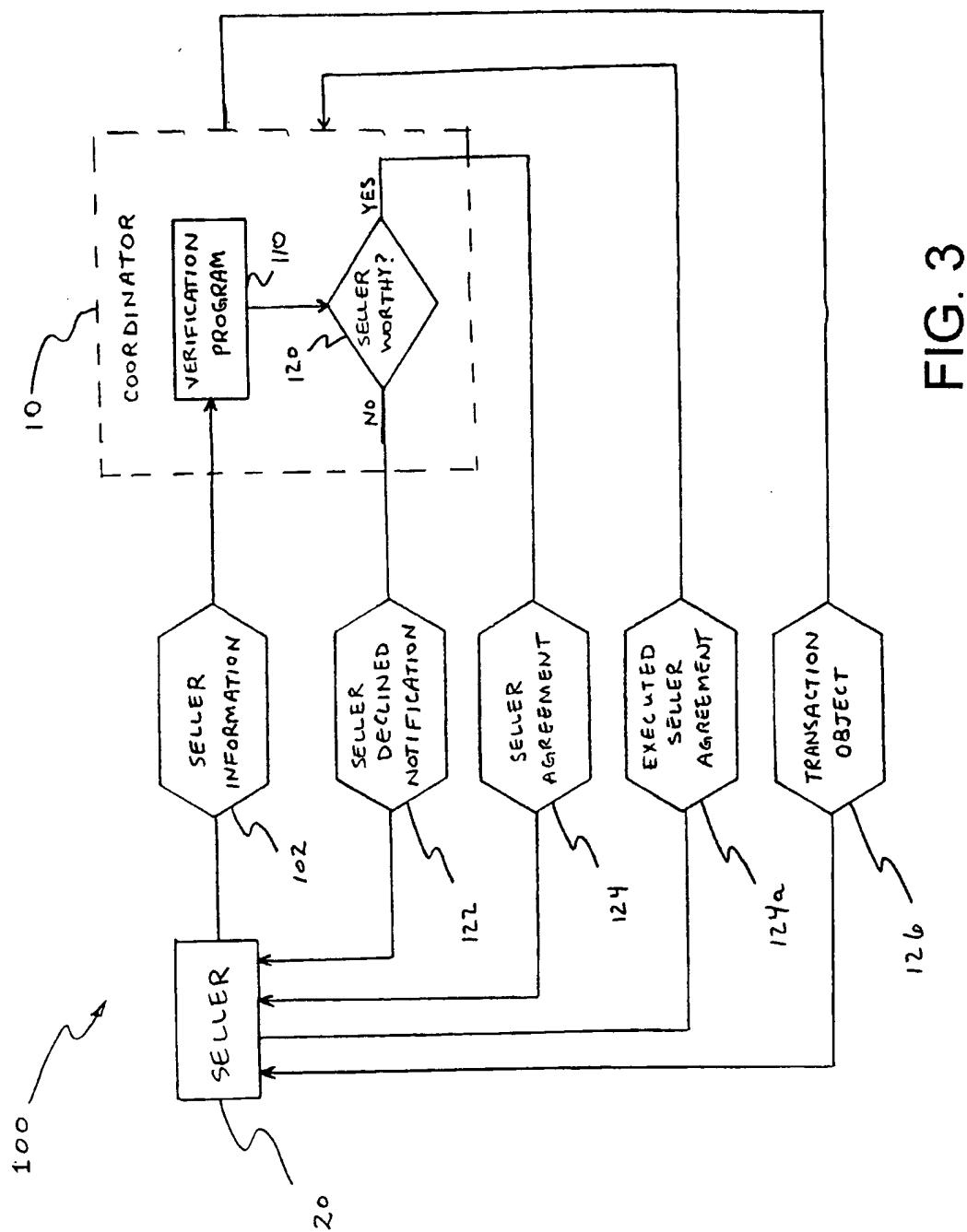


FIG. 3

4/10

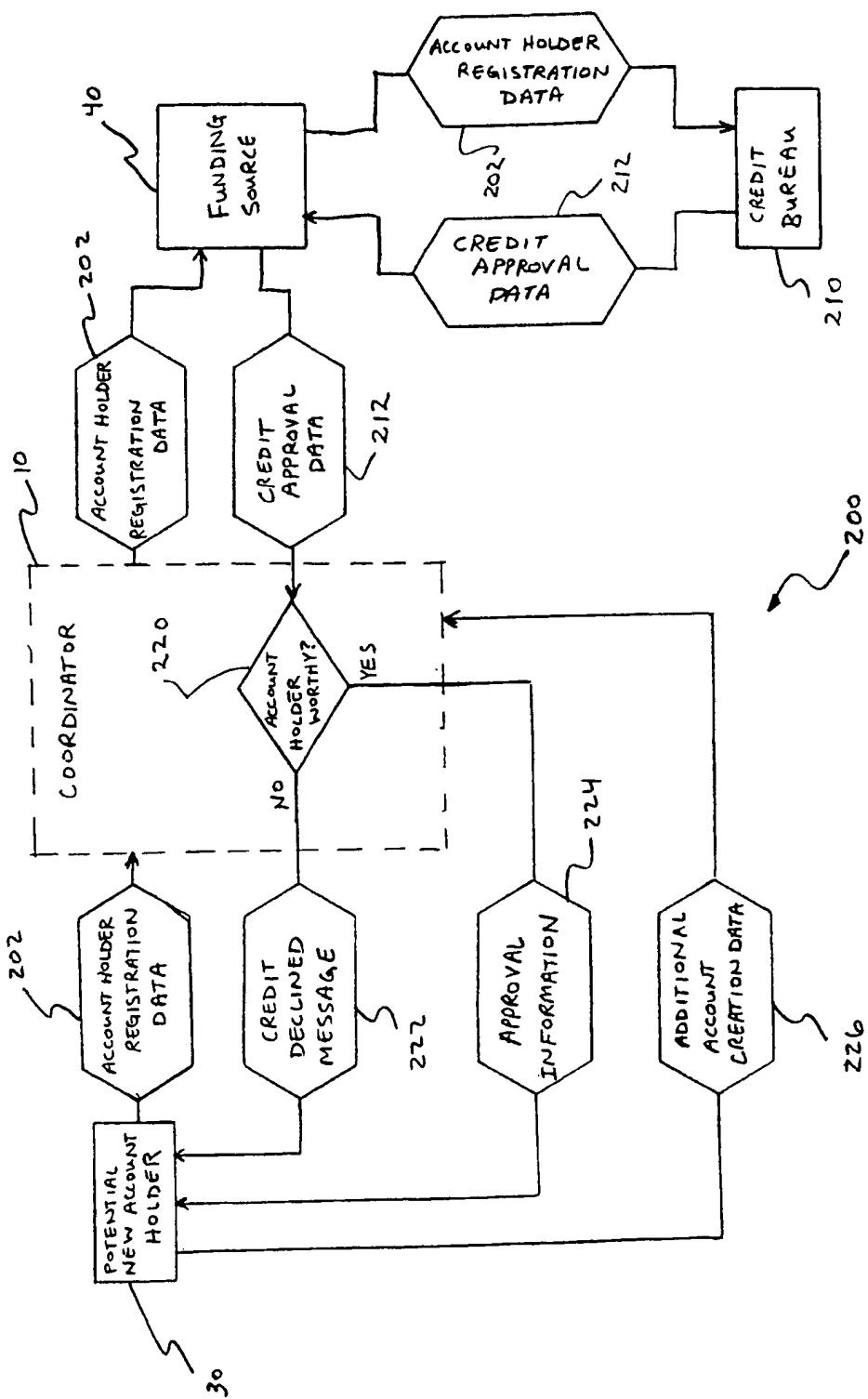


FIG. 4

5/10

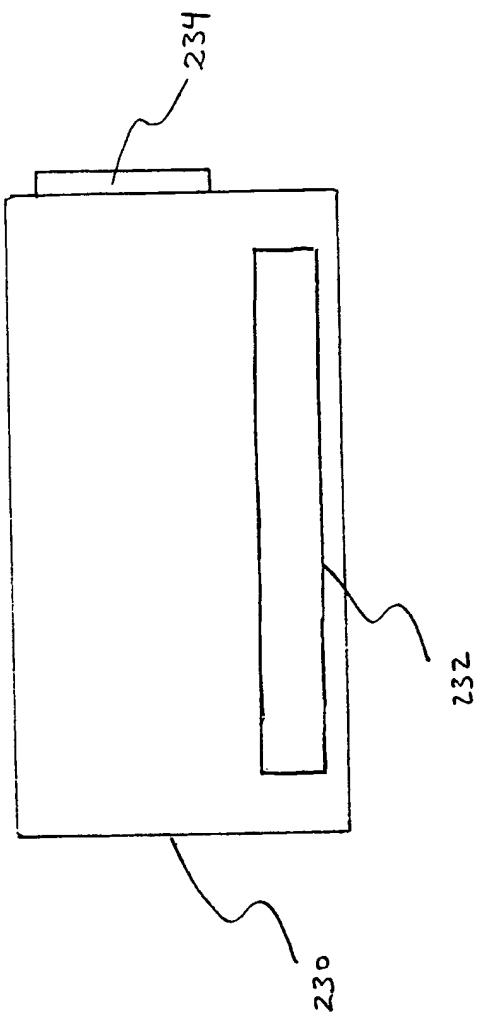


FIG. 5

6/10

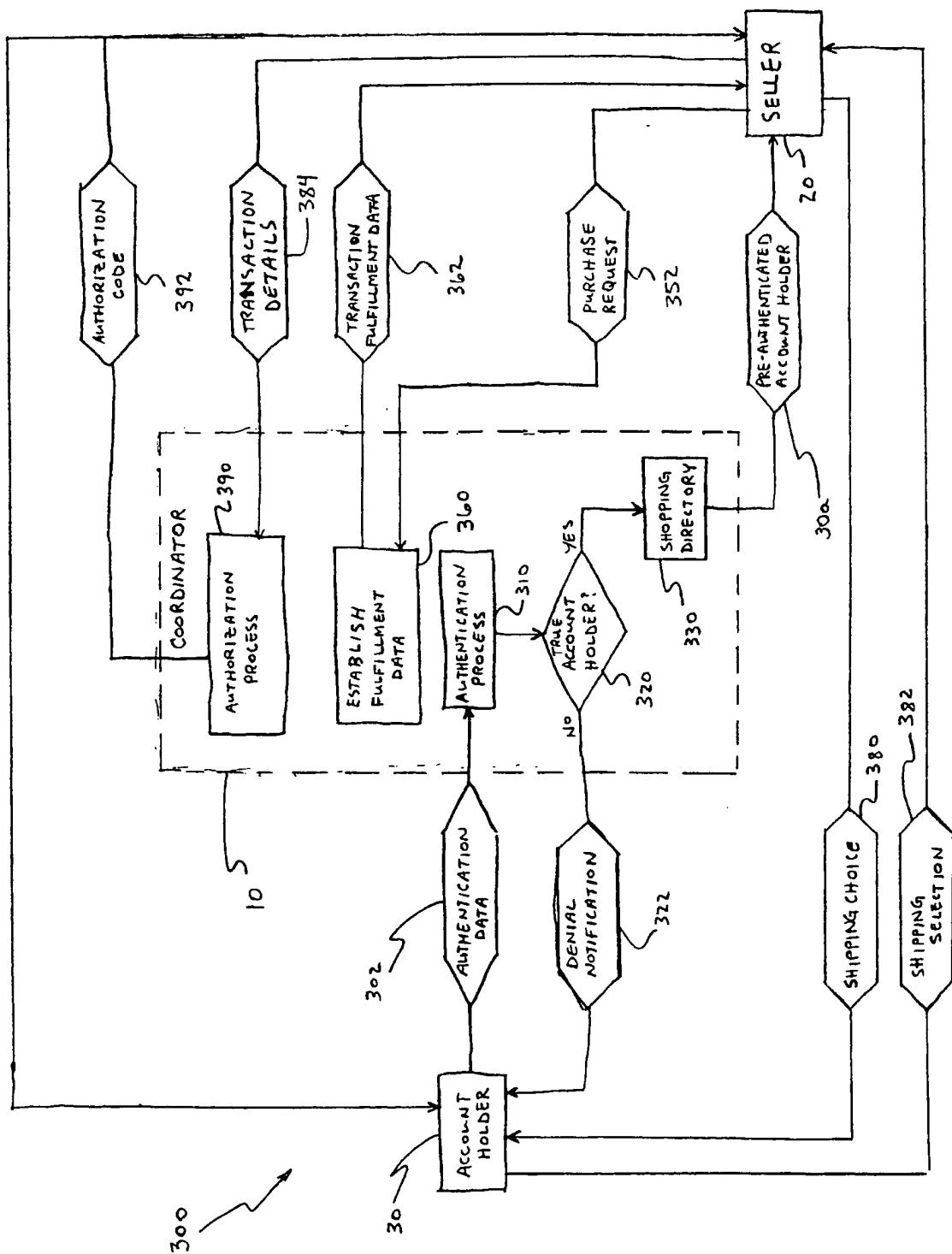


FIG. 6

7/10

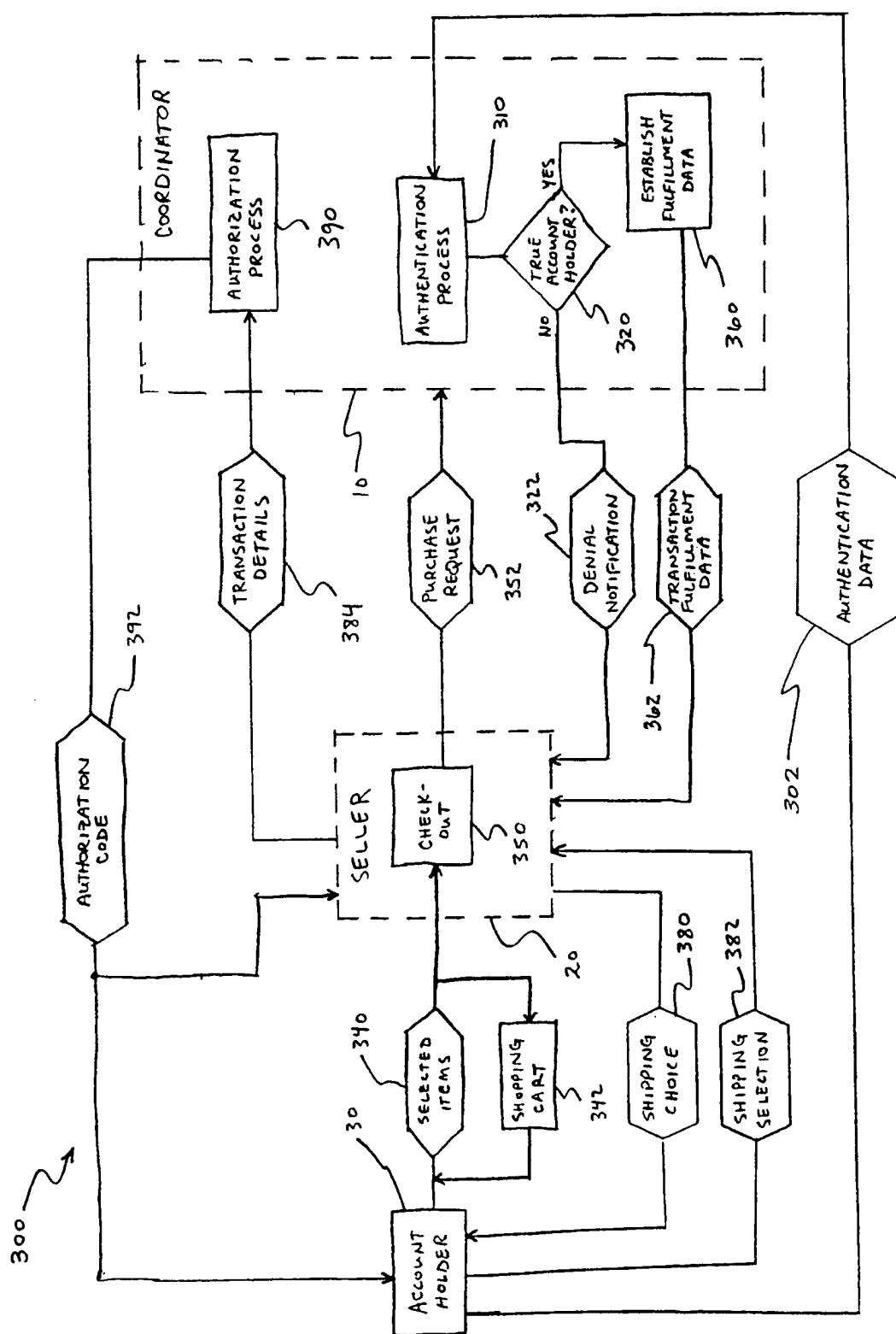
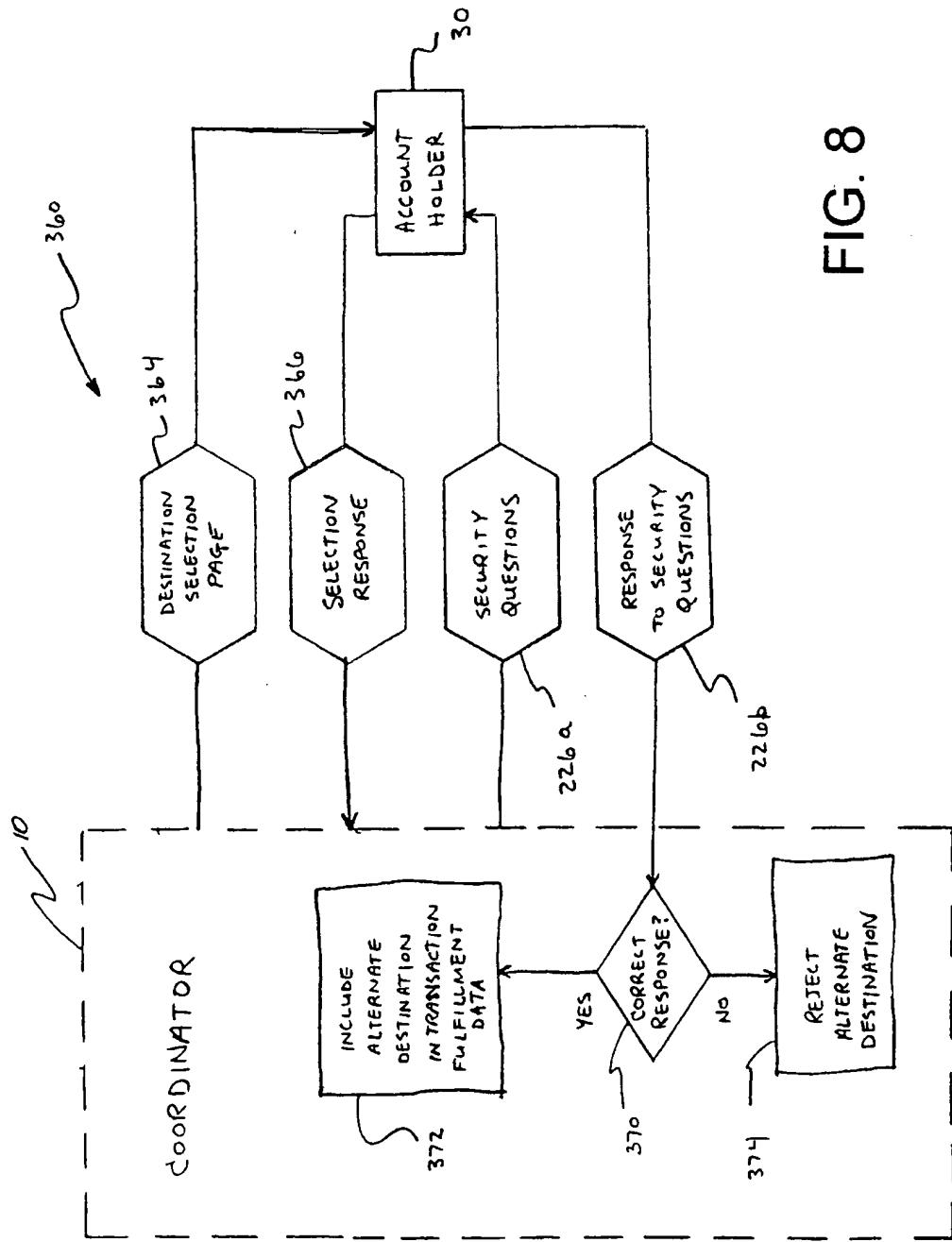


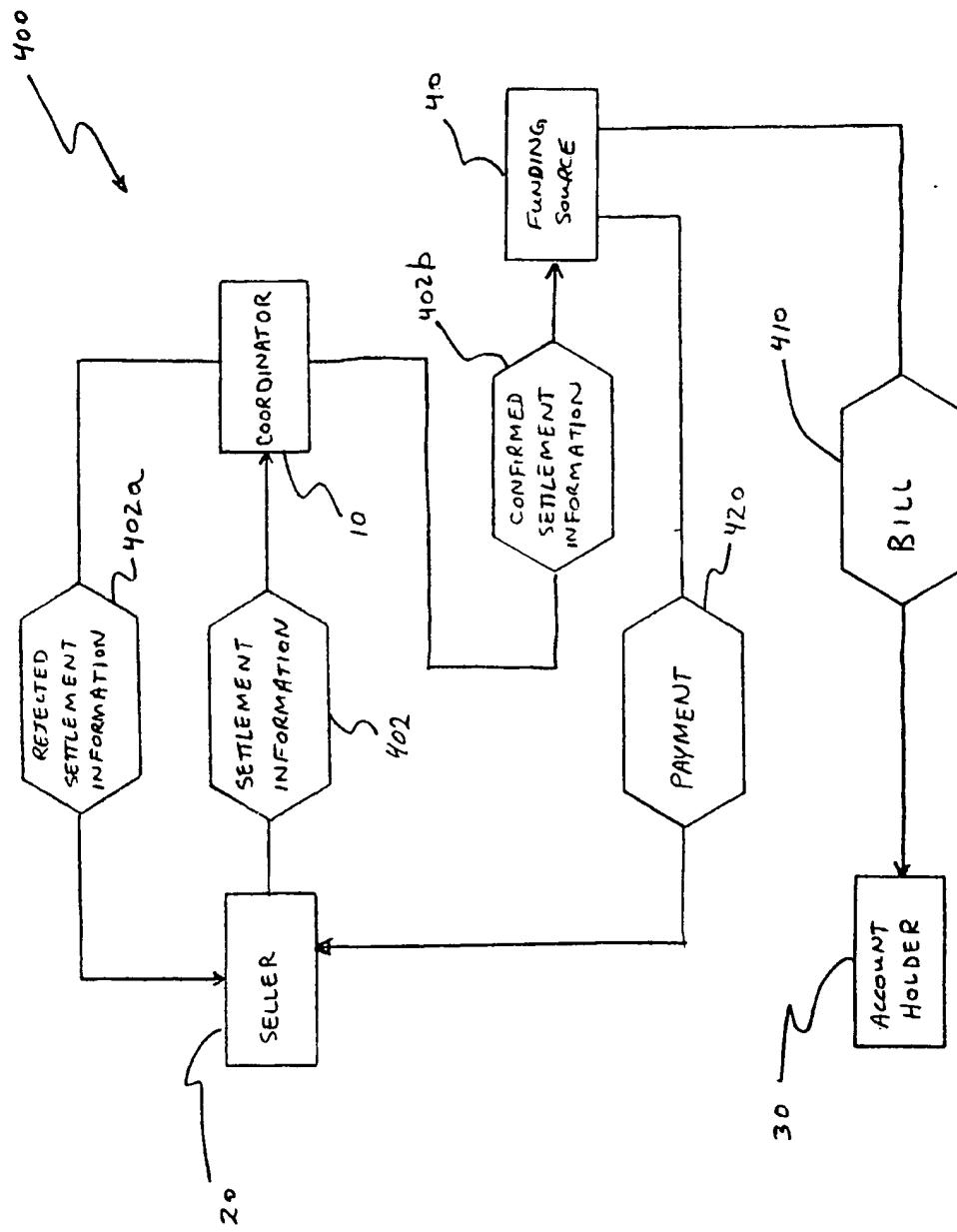
FIG. 7

8/10



9/10

FIG. 9



10/10

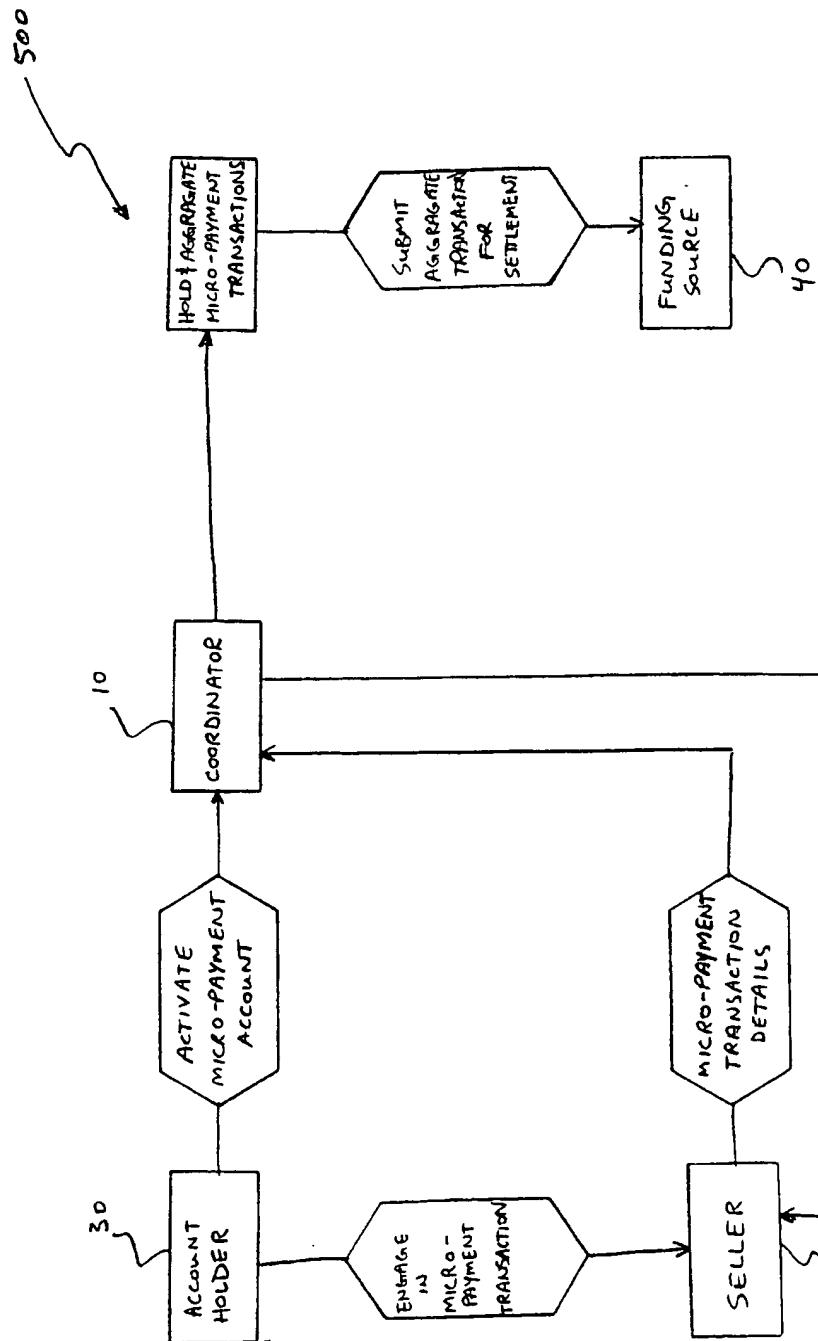


FIG. 10

# INTERNATIONAL SEARCH REPORT

Inte      ional Application No  
PCT/US 00/26965

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G07F G06F H04L G06K G01S G07C H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 93 04425 A (UNIVERSAL PHOTONICS INC) 4 March 1993 (1993-03-04) abstract page 10, line 19 -page 11, line 10 ---	1,2,4,6
Y	EP 0 668 579 A (AT & T CORP) 23 August 1995 (1995-08-23) abstract page 5, line 17 - line 32 ---	1,2,4,6
A	US 4 720 860 A (WEISS KENNETH P) 19 January 1988 (1988-01-19) abstract column 4, line 1 - line 53 column 6, line 50 -column 7, line 61 --- -/-	1,7

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

° Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*&\* document member of the same patent family

Date of the actual completion of the International search

28 February 2001

Date of mailing of the international search report

07/03/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.  
Fax: (+31-70) 340-3016

Authorized officer

Lindholm, A-M

**INTERNATIONAL SEARCH REPORT**

International Application No

PCT/US 00/26965

**C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 491 752 A (KAUFMAN CHARLES W ET AL) 13 February 1996 (1996-02-13) abstract; figures 5,6 column 6, line 46 - line 28 -----	1,7

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Int'l. Application No.

PCT/US 00/26965

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
WO 9304425	A	04-03-1993	US	5537102 A		16-07-1996
EP 0668579	A	23-08-1995	US	5461217 A		24-10-1995
			BR	9500433 A		17-10-1995
			CA	2138829 A		09-08-1995
			CN	1120203 A		10-04-1996
			JP	7319982 A		08-12-1995
			JP	7319983 A		08-12-1995
			US	H1794 H		06-04-1999
US 4720860	A	19-01-1988	US	4856062 A		08-08-1989
			US	4998279 A		05-03-1991
			US	5023908 A		11-06-1991
			US	5168520 A		01-12-1992
			US	4885778 A		05-12-1989
			US	5367572 A		22-11-1994
US 5491752	A	13-02-1996	US	5373559 A		13-12-1994